ORIGINAL RESEARCH PAPER

Computer Science

A NOVEL APPROACH FOR IOT NODE AUTHENTICATION IN MEDIA GATEWAY CONTROL PROTOCOL

KEY WORDS: IoT Security, MGCP, VoIP, Authentication.

Dr.T.Premalatha

Asst.Professor, Dept of Computer Science, VLB Janakiammal College of Arts and Science Kovaipudur, Coimbatore-641042, Tamilnadu.

ABSTRACT

In upcoming days, the numbers of malware is increased against the internet users to collect their privacy details. Smart devices are designed to provide a variety of internet services that range from remotely located personal appliances to wearable or implantable objects. Integrated wireless communications offer the smart devices with novel sensor potential. Heterogeneous communications provides the opportunity to attackers. To protect the communication messages of call agents in media connections, it is essential to encrypt the audio messages against eavesdropping. Gateway session key is acted as the key for encryption. Uncontrolled barge-in is the exact problem of packet networks. This attack can be initiated by directing the media packets to a specific IP address. The packets will be decoded and the signals will be played on the "line side". This attack is focused only from known sources and it slows down the connection establishment. The Call Agent should receive the source address of egress gateway and pass it to ingress gateway for enabling the basic protection. Attacker can obtain the valid pairs of source and destination addresses to create source spoofing attack. The user controls all access points of network against source spoofing. So it is essential to encrypt the packets from the access points by using a secret key to prevent the source spoofing.

I. INTRODUCTION (HEADING 1)

VoIP stands for Voice over IP. It is used to enable the telephones, fax and other communications devices to initiate and receive the calls over a VoIP network. VoIP also worked along with Internet and mobile services to send / receive the voice calls. Media and control signals are used to place a phone call in between the ordinary digital phone network and VoIP network. The voice conversation is done thru the media stream. The dial tones and ring tones are indicating that the call control process is occurring.

A. VoIP Protocols

A VoIP protocol is used to handle three different functions namely call control, gateway control and media control. Call Control signaling is responsible for call setup, search the peer, negotiating the coding protocols, creation and termination of the connection. Gateway control is responsible for controlling the signals between the VoIP gateways. These gateways are negotiating the VoIP traffic on behalf of endpoint phones. The voice or video payload is depends on the Media. Both VoIP networks and ordinary phone networks are used RTP/RTCP. RTP stands for Real-time Transport Protocol and it is used to carry the actual media. RTCP stands for Real Time Control Protocol to carry the status and control information. Endpoints are using the control signals to negotiate the dynamically assigned ports to receive the RTP/RTCP media stream. The Security Gateway is used to protect the VoIP traffic in heterogeneous enterprise environment with the help of Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), H.323 and Skinny Client Control Protocol (SCCP). SIP and H.323 protocols are used in the place of call control signaling process in VoIP gateway. MGCP and SCCP are used in the place of gateway control signaling process. Also, the VoIP gateway used T.120, RTP and RTCP protocols for controlling the audio and video streams. VoIP also makes use of a series of multifaceted protocols that is each one spread potentially vulnerable data throughout many ports. Security Gateway is used to ensure that caller and recipient addresses should be valid for data transfer.

B. VoIP Gateways

The VoIP gateway is classified into two different types of gateways namely analog and digital. The analog VoIP gateway is used to connect customary analog telephones to a VoIP phone system. To accomplish this, the analog VoIP gateway comes in two different forms namely FXS and FXO. FXS gateway stands for Foreign EXchange Subscriber and it is used to connect traditional telephones and fax machines into a VoIP phone system. Also, FXO gateway stands for Foreign EXchange Office and it is used to connect VoIP phone system into PSTN lines. PSTN refers the Public Switched Telephone Network. Digital VoIP gateway is used to connect the VoIP Phone system into digital voice lines such as T1/E1/Basic Rate Interface (BRI) standards. It connects customary Private Branch Exchange (PBX) phone system to an IP network.

VoIP gateways are very strong due to handle the multiple protocols like SIP, H.323 and MGCP. Also, it supports the different voice codec for faxing, cancellation of echo, jitter buffer, Voice Activity Detection (VAD), Comfort Noise Generation (CNG), Web based administration, automatic provisioning through TFTP / HTTP and routing the call to initiate the communication process.

C. Media Gateway

To place the external calls, Cisco Unified Communications Network (CUCM) deployment requests a connection with PSTN. PSTN hook up the customary time-division-multiplexing telephony interface with VoIP domains. Media Gateway Control Protocol (MGCP), H.323 or Session Initiation Protocol (SIP) is used to integrate the CUCM with gateways to perform the signaling operations on VoIP. To provide a different signaling feature, the CUCM is used in MGCP, H.323 and SIP protocols. MGCP used to centralize the dial plan with gateway configuration. H.323 used to configure the dial plan directly on the gateway and also performs third-party integration with service provider network. Also, it used to perform the call routing operations. SIP used to configure the dial plan directly with the gateway and supports the third-party telephony integration with end devices.

D. Media Gateway Control Protocol

MGCP allows the centralized administration of the dial plan to manage the endpoints of devices. CUCM is one of the master/slave protocols like MGCP and Skinny Client Control Protocol (SCCP). To initiate the call signaling process, the MGCP communication is sent to the CUCM for analyzing lookup results of SCCP. CUCM is directly communicating the setup process of SCCP IP phones and MGCP gateways. To manage the IP telephony gateways, MGCP uses call-control devices. CUCM allows the MGCP to get control of exact port on a gateway. MGCP has the benefit of centralized gateway administration. The pre-configured ports of the gateway are controlled thru CUCM. RTP is used in the place of gateway and IP phone and it uses an even port number in the range of 16,384 through 32,767. Also, the endpoint identifiers are addresses the individual endpoint interfaces.

E. Issues in Media Gateway Control Protocol

Any entity in MGCP endpoint may be affected by unauthorized calls. MGCP messages are carried over the secured Internet connections are defined in RFC 2401. The MGCP protocol stack is referred in figure 1.1. The purpose of Gateway is providing the sufficient protection to the endpoints. Also, it provides additional protection in the form of encryption against eavesdropping. It will prevent the monitoring process of third parties.

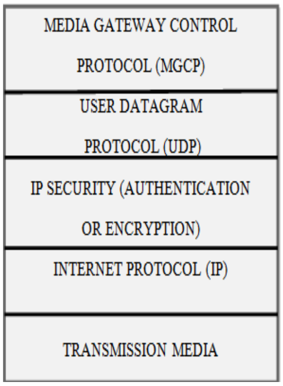

MEDIA GATEWAY CONTROL PROTOCOL (MGCP)
USER DATAGRAM PROTOCOL (UDP)
IP SECURITY (AUTHENTICATION OR ENCRYPTION)
INTERNET PROTOCOL (IP)
TRANSMISSION MEDIA

Figure 1.1 MGCP Protocol Stack Layers

A. Protection of Media Connection

To protect the communication messages of call agents in media connections, it is essential to encrypt the audio messages against eavesdropping. Gateway session key is acted as the key for encryption. Uncontrolled barge-in is the exact problem of packet networks. This attack can be initiated by directing the media packets to a specific IP address. The packets will be decoded and the signals will be played on the "line side". This attack is focused only from known sources and it slows down the connection establishment. The Call Agent should receive the source address of egress gateway and pass it to ingress gateway for enabling the basic protection. Attacker can obtain the valid pairs of source and destination addresses to create source spoofing attack. The user controls all access points of network against source spoofing. So it is essential to encrypt the packets from the access points by using a secret key to prevent the source spoofing.

II. RELATED WORK

Nowadays the smart devices are connected with cloud-computing technologies. Smart devices are needed to balance the storage and computing services [1]. In 2011, the global mobile handset shipments are 1.6 billion units [2] and a total smart phone sale is 472 million units [3]. In reality, in between the year of 2011 to 2012, the numbers of Android OS and iOS users are alone raised from 38 to 84 million according to a report of Nielsen [4]. Also, the report specified that the average numbers of applications per device are raised from 32 to 41. The proportion of time spends by the users on Smartphone applications are approximately equals the time spent on the Web. In addition, the numbers of worldwide Smartphone trade records are saying that a record of 207.7 million units' sale in the year of 2012 and the sales percentage is increase up to 38.3% with compare to the previous year [5]. New smart devices are emerged such as Television [6], Watches [7], Glasses [8], Clothes [9] and Cars [10]. Smart devices are used efficiently in healthcare field to utilize the medical devices such as Smart Pillboxes [11-12] and so on. The new formations of smart wearable systems for health monitoring or implantable medical devices [13] are also included in health care.

Wireless communication technologies are suggested that the smart devices are ubiquitously communicated with an abundant variety of internet services which are remotely located personal appliances or wearable objects. Infrared (IR) and Radio Frequency (RF) communications are the most general technologies utilized by current smart devices. The utilization of IR has moved out unnoticed all through the explosion of Smart phones, but it has become popular again [14]. Wireless communication capabilities for smart devices are used different technologies such as Near Field Communication (NFC), IEEE 802.15.1, EEE 802.11, GSM, UMTS, Radio Data System (RDS), GPS, Software Defined Radio (SDR) and Cognitive Radio (CR). Integrated wireless communications are offered smart devices with novel sensor potentials. The present sensor has growth from mechanical transducers featured with network connectivity to communication-centric systems [15-16]. Some communication techniques are permit the devices to sense their position based on radio signals transmitted thru GPS [17]. The utilization of RFID and NFC in smart devices is to sense the proximity information with the help of programmable tokens or tags [18].

Both Bluetooth smart and SmartTags technologies are used to convert the everyday objects into powerful data sensors to form a number of opportunistic networking paradigms like Device-to-Cloud, Device-to-Device and Device-to-Environment [19]. This technology plays an important role in the communication-based services. Furthermore, the dissimilar communication has provided a useful service like NFC-based epayment schemes, Location-Based Services (LBS) or creates a new form of authentication in anonymous networks [20]. But, the heterogeneous communications provides an opportunity to attackers. Attack vectors have transmitted the new epidemic behaviours [21-23] of malware. One of the most example malware is the arrival of FM radio-based attacks [24]. It is mainly viral due to the broadcast nature of Radio Data System (RDS), Software Defined Radio (SDR) and Cognitive Radio (CR) systems [25] that are dependent on RadioApps. New communication-centric sensors are come up with new privacy problems such as GPS can potentially reveal the user's location and NFC-equipped devices can cause traceability issues. Other accelerometer or gyroscope sensors can exploit the location of screen taps as well as to guess the user passwords. In reality, there are several approaches have occupied in privacy leakage from the sensor's perception [26-27]. For instance, the Smartphone antivirus software detects only 20.2% out of 79.6% malware revealed by Zhou et al. [28]. More hopeful studies like AV-Test [29] are carried out with a limited data set that illustrate 31 out of 41 solutions are offered a low detection rate.

III. PROPOSED METHODOLODY

A. Fuzzy Logic

Fuzzy Logic is used to allow the system implementation small embedded microcontrollers to large networked multi-channel PC control systems. Fuzzy logic provides the easy way of exact conclusion based upon the indefinite information. The powerful mathematical tool is Fuzzy sets. Fuzzy logic is used to model and control the uncertain systems in industry and humanity for estimated the reasoning in judgment making [30-31].

B. Fuzzy Set Theory

The classical set theory is gets extended thru Fuzzy set where the elements have changing their degree of membership. Whenever relating with human reasoning, the logic based on truth values such as true or false is insufficient [32]. To explain the human reasoning, it is essential to use the fuzzy logic. Fuzzy truth represents the membership in unclearly distinct sets. The Members have involved the diverse degree of membership function [33]. A persistent range of truth values in the period notions like quite warm or appealing cold can be formulated mathematically and processed by computers [34].

C. Fuzzification

The process of creating a crisp quantity fuzzy is called as Fuzzification. It can be recognized a lot of quantities to be crisp and deterministic. They will take considerable uncertainty. Due to the imprecision form of uncertainty is considered as the fuzzy variable and can be represented by using membership function [35-36].

D. Defuzzification

Defuzzification is the process of producing a certain result using fuzzy logic is known as fuzzy sets. Equivalent membership degrees are acted as the fundamental in a fuzzy control system. It has a number of rules which transforms a number of variables into a fuzzy set [37].

E. Fuzzy Logic Rules

A decision can be made by using the logic rules and membership sets of fuzzy logic [38]. The decision algorithm uses variable keys to attain both security and low processing. Fuzzification is gets altered based on both key size and the number of mapping tables of the encryption algorithm [39]. The desired key size is fixed by the user and it is range up to 128 bits. The desired key can be entered the form of password. Key is also depends on the number of mapping tables in the algorithm. Allocations of the weights on variables are varying from 0.0 to 1.0 range. The security levels are differing from one to sixteen. A predefined mapping table and the user's initial inputs are used to determine the total number of rounds. The values of mapping tables are mathematically predefined.

F. Implementation of Fuzzy Logic in Media Gateway Network Protocol

The subsequent information like horizontal tab, space, linefeed, colon, full stop and carriage return information is used by the response model of Media gateway. The call agent has numerous queries like Audit Endpoint (AUEP), Audit Connection (AUCX), Connection Creation (CRCX), Connection Deletion (DLCX), Connection Modification (MDCX), Request Notification (RQNT), Endpoint Configuration (EPCF), Notify (NTFY) and Restart in progress (RSIP). These commands are transmitted in the form of three types of security modes like preshared key, raw public key and certificate process. Based on the key, the link has to be recognized and create the secured connection between the nodes.

1) Fuzzy Logic in Blowfish Encryption

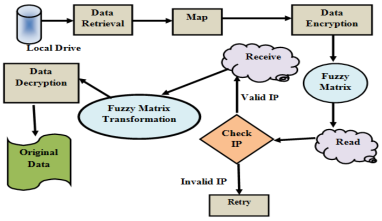


Figure 1.2: Fuzzy Set Theory in Blowfish Encryption

Blowfish algorithm gives a better performance and more secured against any type of intrusion. Blowfish is suitable for the application where the key is not changed often. Also, S-boxes generation of Blowfish are based on the weak key. So it is essential to change the secrecy of key often against the crypt analyst. The proposed system is used a new approach to increase the security of Blowfish algorithm is referred in figure 1.2. Fuzzy logic is implemented in Blowfish's S-boxes stages. The encrypted text's ASCII value is considered for the matrix conversion that ends in binary coded value may be zero or one. Also, the encrypted data is placed into matrix formation to get the fuzzy membership matrix. Matrix transpose formation is utilized at the time of decryption. Encrypted text is converted into matrix format using matrix transpose formation. The fuzzy evaluation score is received at the time of decryption and compared with the predefined key. At the end of the process, the original data can be retrieved without any modifications.

1) Implementation setup

The proposed system is referred as Media Gateway Network Real time Transport Protocol (MGNRTP). MGNRTP has a set of sensor nodes to transfer the information in the form of relay nodes to maximize the life span of constrained nodes. It is interlinked with the master call agent to transmit the packets thru gateway, gateway controller and PSTN. MGNRTP is maintained thru encrypted commands. The entire process of proposed system is specified in Figure 1.3.

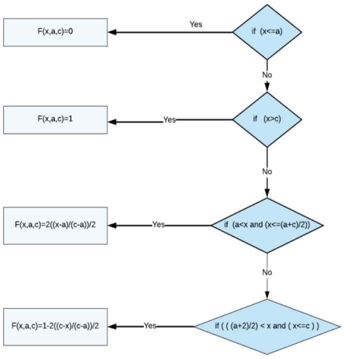

F(x,a,c)=0
Yes
if (x<=a)
No
F(x,a,c)=1
Yes
if (x>c)
No
F(x,a,c)=2((x-a)/(c-a))/2
Yes
if (a<x and (x<=(a+c)/2))
No
F(x,a,c)=1-2((c-x)/(c-a))/2
Yes
if (((a+2)/2) < x and (x<=c))

Figure 1.3: Encryption process of MGNRTP using Fuzzy logic

The proposed system is referred as Media Gateway Network Real time Transport Protocol (MGNRTP). MGNRTP has a set of sensor nodes to transfer the information in the form of relay nodes to maximize the life span of constrained nodes. It is interlinked with the master call agent to transmit the packets thru gateway, gateway controller and PSTN. MGNRTP is maintained thru encrypted commands. The entire process of proposed system is specified in Figure 1.3. The proposed system is used three different stages namely Setup, Encrypt and Decrypt. First, the plain text and secret key has been identified in setup process. Secret key depends on the user's individual identities like password or PIN number that is transformed into the ASCII format for creating the efficient and secure communication. Initially the encrypted text is loaded. With the help of defuzzification, the receiver will decipher the ASCII codes. Then the result is applied to sub-key generation process to obtain the original plain text.

3) Encryption Algorithm

Step 1: Select the Plain Text and Private Key
Step 2: Conversion of Private Key into an ASCII code.
Step 3: Cipher the ASCII codes by using Standard fuzzy functions is referred in Figure 1.3 where x refers ASCII value, a refers the start point and c refers the end point.
Step 4: Convert the result of Fuzzy function into binary stream.
Step 5: Fuzzy values are used as the key to encrypt the given text by using Blowfish encryption algorithm

4) Decryption Algorithm

Step 1 : Load the Encrypted Text.
Step 2 : Enter the Secret Key to Decipher the ASCII codes using the equation 1.1.

$$\text{Output}=\frac{\sum_i \mu_a(y_i)*y_i}{\sum_i \mu_a(y_i)} \xrightarrow{\qquad} \text{Equation 1.1}$$

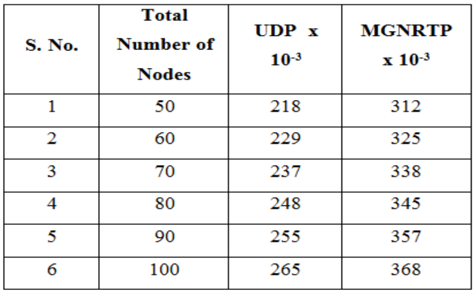
Where μA and yi is a parameter of inverse fuzzy function.

Step 3 :Apply result into sub-key generation.
Step 4 :Apply Round function of Blowfish Algorithms.
Step 5 :Get the Orginal Plain Text

VI. EXPERIMENTAL RESULTS AND DISCUSSION

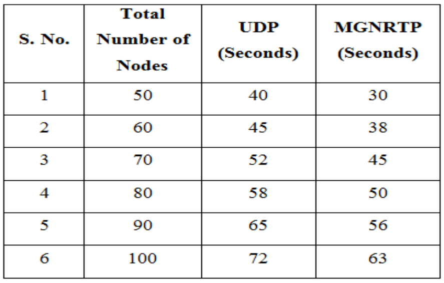
The proposed methodology is implemented in NS2 simulator. It uses 802.5.14 low energy wireless communication standard protocol. It utilizes the different ranges of frequency bands such as 800MHZ, 900 MHZ and 2.4 GHZ. It fixes the simulation area of NS2 simulators as 250m2, transmission rate as 250kbps, channel modes as log shadowing wireless model, packet size as 40 bytes and the number of nodes ranges from 50 to 90. The proposed MGNRTP with fuzzy based blowfish encryption process is compared with traditional User Datagram Protocol(UDP). The evaluation parameters of both proposed and existing protocols are based on the delay, energy consumption and throughput.

Table 1.1 Energy consumption between UDP and MGNRTP



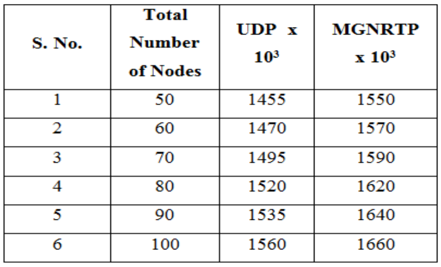
S. No.	Total Number of Nodes	UDP x 10^{-3}	MGNRTP x 10^{-3}
1	50	218	312
2	60	229	325
3	70	237	338
4	80	248	345
5	90	255	357
6	100	265	368

Table 1.2 Life span between UDP and MGNRTP



S. No.	Total Number of Nodes	UDP (Seconds)	MGNRTP (Seconds)
1	50	40	30
2	60	45	38
3	70	52	45
4	80	58	50
5	90	65	56
6	100	72	63

Table 1.3 Throughput values for UDP and MGNRTP



S. No.	Total Number of Nodes	UDP x 10^3	MGNRTP x 10^3
1	50	1455	1550
2	60	1470	1570
3	70	1495	1590
4	80	1520	1620
5	90	1535	1640
6	100	1560	1660

The energy, lifespan and throughput of different nodes using proposed MGNRTP with fuzzy based Blowfish protocol and traditional UDP protocol is depicted in table 1.1.,1.2 and 1.3. The results show that the proposed methodology attains high packet delivery ratio up to 1660 packets for 100 nodes. It implies that it handles the intermediate attacks using fuzzy based encryption process in an efficient manner. The life span of proposed methodology increases up to 63seconds for 100 nodes due to low energy. The low energy consumption always increases the life span of constrained nodes. The results show the proposed methodology consumes low energy, increases the life span of nodes and maximum throughput of the nodes.

V. CONCLUSION

This paper analyzes the heterogeneneous media communication process in IoT devices. The call agent use Media Gateway Network Real time Transport Protocol(MGNRTP) for initiating the media connection as well as control messages. Due to heterogeneous communication, the MGNRTP needs protection against Denial of Service (DoS) attack. This paper suggested a new fuzzy based blowfish symmetric encryption algorithm for node authentication. The proposed methodology is simulated in NS2 and compared with the traditional User Datagram Protocol(UDP). The results show that media communication process in heterogeneous environment of IoT devices consumes low energy, high packet delivery ratio and maximum life span period as compared with UDP.

REFERENCES

[1] H. Dediu, "When will tablets outsell traditional pcs?" March 2012. Available: http:// www. asymco. com / 2012/03/02/ when-will-the-tablet-market-be-larger-than-the-pc-market/.

[2] Juniper, "2011 mobile threats report", Juniper Networks, Tech. Rep., February 2012

[3] L. Goasduff and C. Pettey, "Gartner says worldwide smartphone sales soared in fourth quarter of 2011 with 47 percent growth", Visited April 2012, http://www.gartner.com /it /page.jsp?id=1924314.

[4] Nielsen, "State of the appnation -a year of change and growth in u.s. smartphones," Nielsen, Tech. Rep, March 2012.

[5] van der Meulen, R., & Rivera, J. (2013). Gartner says worldwide mobile phone sales declined 1.7 percent in 2012," Visited March 2013. Avalialbe :http://www.gartner.com /newsroom/id/2335616.

[6] http:// www.samsung.com / us /2012-smart-tv/

[7] http:// www.sonymobile.com/us/products/accessories /smartwatch/

[8] http://www.google.com/glass/

[9] http://www.cutecircuit.com/tshirtos-the-future-is-getting-closer/

[10] http://www.wired.com/autopia/2013/03/weblink-abalta-auto-apps/

[11] S. Larner, "Smartphones and tablets in the hospital environment", British Journal of Healthcare Management, Volume:18, Issue: 8, PP: 404–405, August 2012.

[12] http://www.innovatorsinhealth.org/solutions/

[13] M. Chan, D. Estve, J.-Y. Fourniols, C. Escriba, and E. Campo, "Smart wearable systems: Current status and future challenges", Artificial Intelligence in Medicine, Volume:56, Issue:3, PP:137 – 156, November 2012.

[14] D. Seifert."Back from the dead: why do 2013's best smartphones have IR blasters?", April 24, 2013. [Online]. Available: http://www.theverge.com/2013/4/24/4262074/is-this-the-year-of-the-ir-blaster

[15] F. Wang and J. Liu, "Networked wireless sensor data collection: Issues,challenges, and approaches", IEEE Communications Surveys & Tutorials, Volume: 13, Issue:4, PP:673–687, November 2011.

[16] Ye Yan, Yi Qian, Hamid Sharif, David Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", IEEE Communications Surveys & Tutorials, Volume:15, Issue:1, PP:5 - 20, February 2013.

[17] Yanying Gu , A. Lo , I. Niemegeers, "A survey of indoor positioning systems for wireless personal networks", IEEE Communications Surveys & Tutorials, Volume:11, Issue:1, PP:13–32, January 2009.

[18] C. MacManus. "Sony's smarttags could change phone habits", Januray 16,2012 [Online]. Available: https://www.cnet.com/news/sonys-smarttags-could-change-phone-habits/

[19] Lee, Y., Ju, Y., MIN, C., YU, J., & Song, J,"MobiCon: Mobile context monitoring platform: Incorporating context-awareness to smartphone-centric personal sensor networks", Institutional Knowledge at Singapore Management University, PP:109–111, June 2012

[20] D. Kelly, R. Raines, R. Baldwin, M. Grimaila, and B. Mullins, "Exploring extant and emerging issues in anonymous networks: A taxonomy and survey of protocols and metrics", IEEE Communications Surveys & Tutorials, Volume:14, Issue:2, PP:579–606, June 2012.

[21] C. Szongott, B. Henne, and M. Smith, "Evaluating the threat of epidemic mobile malware", in Proceedings of IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2012), PP:443–450, October 2012.

[22] La Polla, M. and Martinelli, F. and Sgandurra, D., "A Survey on Security for Mobile Devices", IEEE Communications Surveys & Tutorials, Volume:15, Issue:1, PP:446–471, February 2013.

[23] X. Wei, N. C. Valler, B. Prakash, I. Neamtiu, M. Faloutsos, and C. Faloutsos, "Competing memes propagation on networks: A network science perspective" ,IEEE Journal Selected Areas in Communication s, Volume:31, Issue:6, PP:1049–1060, June 2013.

[24] Fernandes, Earlence and Crispo, Bruno and Conti, Mauro, "FM 99.9, Radio Virus: Exploiting FM Radio Broadcasts for Malware Deploymen", IEEE Transactions on Information Forensics and Security, Volume:8, Issue:6, June 2013.

[25] Gianmarco Baldini , Taj Sturman , Abdur Rahim Biswas , Ruediger Leschhorn , Gyozo Godor , Michael Street , "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead", IEEE Communications Surveys & Tutorials, Volume:14, Issue:2, PP:355–379, May 2012.

[26] S. Amini, J. Lindqvist, J. Hong, J. Lin, E. Toch, and N. Sadeh, "Cache: caching location-enhanced content to improve user privacy", in Proceedings of 9th International Conference on Mobile systems, applications, and services, ACM, PP:197–210, June 2011.

[27] A. Parate, M.-C. Chiu, D. Ganesan, and B. M. Marlin, "Leveraging graphical

models to improve accuracy and reduce privacy risks of mobile sensing", in Proceedings of 11th International Conference on Mobile Systems, Applications and Services,ACM,PP:83–96,June 2013.
[28] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution", in Proceedings of 33rd IEEE Symposium Security and Privacy (Oakland 2012), PP:95-109,May 2012.
[29] AV-TEST GmbH, "Anti-Malware solutions for Android",March, 15th 2012
[30] Zadeh, L. A.,"Fuzzy Sets and Applications: Selected Papers",John Wiley, New York, 1987
[31] Dhenakaran, S. S., & Kavinilavu, N. "A New Method For Encryption Using Fuzzy Set Theory",Tianjin: Tianjin Science & Technology Publishing House, PP:37-101, 1990
[32] Shafi Golgwasser Mihir Bellare, "Lecture Notes on Cryptography", July 2008
[33] Le Luo, "A method of quality evaluation of hydropower project based on fuzzy mathematics", Journal of Huazhong University of Science and Technology,Nature Science Chinese Edition,Volume:32,Issue:8,PP:82-84,2004.
[34] Bonde, A., "Fuzzy logic basics",Site Terrific Web Solutions GTE2194,2000.
[35] N. H. Mateou ,A. S. Andreou ,George A. Zombanakis,"Fuzzification and Defuzzification Process in Genetically Evolved Fuzzy Cognitive Maps (GEFCMs)", 8th WSEAS International Conference on Circuits, Systems, Communications and Computers (CSCC),PP:1-4,July 2004.
[36] Timothy J. Ross, "Fuzzy Logic with Engineering Applications", Second Edition, 2004.
[37] http://en.wikipedia.org/wiki/Defuzzification
[38] L.A. Zadeh, ed. R.R. Yager et al,"Fuzzy Sets and Applications: Selected Papers", John Wiley, New York, 1987.
[39] "U.S. Loses Focus on Fuzzy Logic", Machine Design, June 21, 1990